IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Thomas Michael Gil et al.	Art Unit	: 2155
Serial No.	: 09/931,223	Examiner	: Nawar, Asad M.
Filed	: August 16, 2001	Conf. No.	: 2855
Title	: STATISTICS COLLECTION FOR NETWORK TRAFFIC		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

At the outset Appellant clarifies the conclusion stated in Appellant's Appeal Brief. Appellant stated: "Appellant submits, therefore, that Claims 1-30 and 32 are allowable over the cited art." Appellant intended to state however that: "Appellant submits, therefore, that Claims 1-21 and 50-77 are allowable over the cited art."

Pursuant to 37 C.F.R. §41.41, Applicant responds to the Examiner's Answer as follows:

35 U.S.C. §112 ¶2 Rejection

Appellant notes that the amendment has been entered and that the rejection has been overcome.

35 U.S.C. §102(b) Rejection

In prefatory remarks to answer Appellant's arguments over Lyle, the examiner states: "It should also be noted that numerous claim limitations argued by the appellant are not present in all independent claims (i.e. the claims are not parallel as some independent claims may not have the argued limitation or it may be presented as a dependent claim)."[1] Appellant responds that it is unfortunate that the examiner has chosen to address Appellant's arguments without regard to individual claims or claim groupings. For each claim argued in the Appeal Brief, Appellant argued only those features that appeared in the claim that was presented for argument. Appellant

[1] Examiner's Answer page 11.

CERTIFICATE OF MAILING BY EFS-WEB FILING

I hereby certify that this paper was filed with the Patent and Trademark Office using the EFS-WEB system on this date: August 30, 2007

has not argued features that do not appear in the claims argued, as the examiner appears to suggest.

The examiner also contends that: "Appellant argues: Lyle neither describes nor suggests producing statistics corresponding to a parameter of traffic flow (Argument A-see brief page 10). *** Furthermore, it should be noted that most of the independent claims do not mention this limitation and if they do, it is presented in the preamble."[2] Appellant contends that this contention is erroneous. Each of Appellant's independent claims[3], as well as several of Appellant's dependent claims, mention the limitation of "statistical information" in the body of the claim either as "producing statistical information ..." or "accumulate statistics from the packets."

Therefore, in Reply to the Examiner's Answer, Appellant maintains the groupings established in the Appeal Brief to the extent possible.

2. Claims 63-68 and 70-75 are not anticipated by Lyle et al (US 6,971,028).

Claims 63, 66, 70 and 73

In Claim 63, Appellant argued the features of ... producing statistics corresponding to a parameter of the traffic flow to trace a source of an attack, with producing further comprising, mapping the traffic flow into a plurality of buckets, varying the number of buckets according to the amount of traffic and number of flows to breakdown traffic flow into different buckets and analyzing statistics accumulated for a parameter and a corresponding threshold in the bucket to identify the source of the attack.[4]

---

[2] "This limitation" is taken by Appellant to be "producing statistics corresponding to a parameter of traffic flow to trace the source of an attack."

[3] Claim 1 recites: "producing statistics corresponding to a parameter of traffic flow to trace the source of an attack." Claim 14 recites: "accumulate statistics from the packets." Claim 21 recites: "accumulate statistics from the packets." Claim 63 recites: "producing statistics corresponding to a parameter of the traffic flow to trace a source of an attack." Claim 70 recites: "produce statistics corresponding to a parameter of the traffic flow to trace a source of an attack."

[4] "Claim 63 includes the features of producing statistics corresponding to a parameter of traffic flow to trace the source of an attack. According to claim 63 producing includes mapping the traffic flow into a plurality of buckets and varying the number of buckets according to the amount of traffic and number of flows by breaking down traffic

The examiner, in Answer, argues that: "In response, the examiner agrees the appellant that "the sniffer 'continuously scans the data being received at various ports of various network devices." Appellant did not argue this.[5]

The thrust of the examiner's argument is that Lyle uses the sniffer module to monitor network traffic and gather information which the examiner "equates" to the claimed statistical information and uses this "information" to yield a parameter indicating a suspected or actual attack.[6]

Claim 63 is directed to a method of monitoring network traffic. The patentable features of producing statistics corresponding to a parameter of the traffic flow ... by varying the number of buckets according to the amount of traffic and number of flows, provides the disclosed advantage and a motivation for the invention, of making the method of producing the statistics less susceptible to denial of service attacks.[7]

Lyle describes sniffers. According to Lyle, "... the sniffer module 304, referred to above, which is used to monitor network traffic at the ports of devices throughout the network, one or more ports at a time, to identify messages related to a known or suspected attack or to

---

flow into different buckets and examining statistics accumulated for a parameter and a corresponding threshold in the bucket.

[5] Rather, Appellant argued that: "Lyle merely uses sniffers, but according to Lyle, the sniffer "continuously scans the data being received at various ports of various network devices. The sniffers search for data indicating an actual or suspected attack, as described more fully below, and provide information concerning suspicious data to other modules within the tracking system, as described more fully below." [Lyle Col. 7, Lines 7-12]."

[6] (col 7, lines 7-12 and 32-42).

[7] Disclosed advantage on page 15, line 3:

> An attack designed to use the algorithm of FIG. 6 against a gateway 26 or a data collector 28 might send packets in such a fashion as to explode the number of buckets. Since each bucket consumes memory space, the attack can be designed to consume all available memory and crash the device, e.g., computer on which the monitoring process 32 executes. There are ways of preventing that type of attack on the monitoring process 32. ***
>
> Referring to FIG. 8, a second method is that instead of using just thresholds and values inside a given bucket, the monitoring process 32 also sets thresholds on the number of buckets. ***
>
> The function of the variable number of buckets is to dynamically adjust the monitoring process to the amount of traffic and number of flows, so that the monitoring device (e.g., gateway 26 or data collector 28) is not vulnerable to DoS attacks against its own resources. The variable number of buckets also efficiently identifies the source(s) of attack by breaking down traffic into different categories (buckets) and looking at the appropriate parameters and thresholds in each bucket.

identify messages that satisfy certain pre-configured criteria believed to indicate the likelihood or possibility that an attack is taking place."[8]

Appellant contends that sniffers examine messages that have the characteristics of a known attack.[9] Lyle does not disclose the sniffers as collecting "statistics accumulated for a parameter." Therefore, there exists no basis for the examiner to argue that: "When the information (statistics) has been gathered and yields a parameter indicating a suspected or actual attack, appropriate action is taken (col 7, lines 7-12 and 32-42)." Sniffers as taught by Lyle, do not gather statistics corresponding to a parameter of the traffic flow to trace a source of an attack.

The examiner inadvertently acknowledges the distinction between "statistics accumulated for a parameter" and identifying messages related to a known or suspected attack when the examiner argues: "In response, the examiner points out that events as described by Lyle's disclosure pertain to traffic flows that correspond to suspicious data."[10] In Lyle, suspicious data is data identified in a messages that is related to a known or suspected attack. Accordingly Lyle and by inference the examiner acknowledges a distinction between "statistical information" and the gathered information taught by Lyle.

The examiner also argues that: "Appellant's claims are broad and thus interpreted as such."[11] Appellant responds that the claims are as broad as Lyle and the other cited art allows the claims to be.

The examiner also argues that:

---

[8] Lyle col. 7, lines 33-38.

[9] Id. Col. 7, line 9; See also Col. 10, lines 21-36.

> With respect to both switch and router traffic, the sniffer module searches a high volume of network traffic looking for any indication that an attack may be taking place. For example, the sniffer module may search for strings that match pre-defined strings considered suspicious, such as strings associated with known types of attacks or particular prior attacks.
>
> The sniffer module may also search for other information, clues, or signatures previously associated with attacks on the network being protected or other networks. For example, the sniffer module may identify all messages sent from one of a list of suspicious source addresses, or messages attempting to access a target system within the network or sub-network associated with the tracking system via a service known to be vulnerable, such as telnet, or messages containing strings present in messages associated with prior attacks.

[10] Examiner's Answer page 12

[11] Id. page 11.

> ***** These traffic flows are placed in events or buckets and are placed in queues for further analysis (col 7, lines 43-58). In light of the above clarification, it should be apparent that all limitations as positively claimed are explicitly and set forth in the Lyle disclosure. Furthermore, the examiner notes that nowhere in the claims, independent or dependent, is there a recitation that the traffic flow must contain an entire set of packets starting from point X and ending at point Y. Therefore, there is no limitation on the size of the flow. It could essentially be a single packet at a port egress or ingress. Therefore Lyle meets the scope of the limitations as currently claimed.[12]**

The thrust of the issue before the Board is whether the examiner's characterization of Lyle's teaching "These traffic flows are placed in events or buckets and are placed in queues for further analysis (col 7, lines 43-58).", corresponds to the features of "mapping the traffic flow into a plurality of buckets and varying the number of buckets according to the amount of traffic and number of flows to breakdown traffic flow into different buckets."

Appellant contends that event data placed in queues, as disclosed by Lyle do not correspond to the claimed buckets, or varying of the number of buckets according to traffic and number of flows. Lyle describes:

> **When information related to an actual or suspected attack is received by the handoff receiver 302 or identified by the sniffer module 304, the relevant information is provided to an event manager module 306. The event manager 306 receives the suspicious data, referred to herein as "event" data, places it in a queue, and provides data to the analysis framework module 308 for processing, one event at a time, at predetermined intervals. The event manager 306 also supplies event data to the log database 320 as it is received either from the handoff receiver 302 or from the sniffer module 304. The event data stored in log database 320 may then be used for post-attack analysis or it may be shared with other tracking systems installed in the same administrative domain in which the tracking system in which the event manager 306 is located, or with tracking systems in other administrative domains, as described more fully below.[13]**

It is clear from this description that Lyle is directed to placement of events, which Lyle describes as pre-defined strings considered suspicious, such as strings associated with known types of attacks or particular prior attacks or clues, or signatures,[14] into queues for processing. However, if the queues described by Lyle were in fact the buckets, as claimed by Appellant, then Lyle would not also describe processing one event at a time.[15] Processing one event at a time

---

[12] Examiner's Answer page 12.
[13] Lyle Col. 7, lines 43-58.
[14] See fn 8.
[15] Id. Col. 7, line 49.

would have no relevance to the claimed buckets and the feature of: "analyzing statistics accumulated for a parameter."

Lyle describes the queue as:

> **FIG. 6 illustrates a queue table 600 used in one embodiment to queue events to be sent to the analysis framework. The columns in table 600 are identified by a column address number between 0 and 6 and the rows are identified by a row address number between 0 and 2. Certain of the cells of table 600 contain one or more letters between A and G, each letter representing an event. For example in the queue at row 0, column 1, three events identified by the letters A, B, and C are being held. By contrast, the adjacent cell at row 0, column 2 does not contain any events in the queue associated with that cell.**

Lyle discloses that each cell can hold multiple events, thus each cell has multiple entries, since Lyle also discloses that the events are processed one at a time.[16]

With respect to the feature of varying, the examiner argues:

> In response, the examiner agrees with the appellant that Lyle teaches that events that are not related to any other events are associated with a new incident object. Contrarily, events corresponding to an existing event or group of related events are aggregated or combined into a single event. Furthermore, Lyle teaches that as the traffic increases new events are created to accommodate new incidents. However if the traffic corresponds to an existing event, the events will be combined to save resources. Also, event rates and flows received close in time in the same network are taken into consideration when creating/dividing/aggregating an event (Col. 13, lines 19-59). Therefore Lyle meets the scope of the limitation as currently claimed.[17]

The examiner's response is a mischaracterization of what Appellant argued.[18] The examiner also mischaracterizes Lyle as teaching that events are "aggregated into a single event"

---

[16] Lyle Col. 7, lines 46-51. "The event manager 306 receives the suspicious data, referred to herein as "event" data, places it in a queue, and provides data to the analysis framework module 308 for processing, one event at a time, at predetermined intervals. The event manager 306 also supplies event data to the log database 320 as it is received either from the handoff receiver 302 or from the sniffer module 304. The event data stored in log database 320... ."

[17] Examiner's Answer

[18] Appellant argued:

> Lyle merely teaches to associate related events. Lyle teaches: "The analysis framework 308 associates the event data with an event software object, as described more fully below, and stores data relating to the event in an event database 322. The analysis framework 308 also determines whether an event is associated with an existing event or group of related events, and associates related events into a single incident software object. Events that are not related to any other events are associated with a new incident object and may be later grouped with subsequently-received event data that is related to the same incident." [Lyle col.7, Line 61 to Col. 8 line 4]

Lyle does not mention that events are aggregated or combined or any equivalent process. Rather, Lyle discloses that events which are related are "associated." By "associated" Lyle means that the events are noted as "related." Otherwise where events added together in Lyle there would be no way to process the event one at a time or look for suspicious strings, clues, and signatures, since all of the data would be lost or obscured.

In essence, the examiner's entire rationale amounts to an unsupportable and legally improper[19] modification of Lyle that would either have Lyle process statistical information on packet flows, rather than processing suspicious strings, clues, and signatures, as disclosed in Lyle or processing what would be – garbage – the obvious outcome if "associating events" corresponded to accumulating events into a queue as a single event, as the examiner argues. Accumulating events into a queue, as argued by the examiner, would destroy all of the information that Lyle seeks to process.

Accordingly, since Lyle fails to describe all of the features of claim 63 arranged as in the claim, Lyle cannot anticipate claim 63.

Claims 64, 66, 68, 71, and 75

Claim 64 was argued as representative of this group of claims. Claim 64 further limits claim 63 and recites that: "varying varies the number of buckets so that the monitoring device is not vulnerable to DoS attacks against its own resources." This feature is not described by Lyle.

The examiner responds that:

> **"... Lyle clearly indicates that its method provides strong protection and is robust against DoS attacks (col 19, lines 37-45). Throughout the disclosure, Lyle describes its method as a protocol. For example, in the same column in question (col 19), Lyle describes his method in Figure 11 A and then continues by saying, "The communication protocol described above is advantageous because it..." Similarly,**

[19] The examiner so construes Lyle so as to modify the teachings of the reference which is clearly improper in the context of a rejection under 35 U.S.C. 120(b). The examiner has not argued inherency but instead seeks to change the principal of operation of Lyle.
It is well settled in the context of an obviousness rejection that:

> If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. *In re Ratti, 270 F.2d* 810, 123 USPQ 349 (CCPA 1959).

Appellant contends that it is clearly improper for the examiner to modify a reference in the context of an anticipation rejection when such a modification would be improper were the claims rejected as obvious.

> **Lyle shows that his method is robust against DoS. So therefore, Lyle disclosure including the varying of the number of buckets provides the intended protection against DoS attacks.**

The examiner conflates two different teachings in Lyle. When Lyle describes that "its method provides strong protection against DoS attacks," Lyle is referring to the communication protocol.[20] The portion of the teachings relied on in Lyle by the examiner to teach buckets, etc. namely, Lyle's event queuing, is not described by Lyle as strong against DoS attacks. Therefore, because it is the communication protocol and not the event tracking system itself that protects the event tracking system, requiring that the would be attacker both "know the communication protocol and have the cryptographic hash function being used as part of the communication protocol."[21], it is submitted that the features of the claim are neither described nor suggested by Lyle.

Claims 65 and 72

Claim 65 was representative of this group of claims. Claim 65 includes the feature that varying the number of buckets includes comparing the number of buckets to a threshold number of buckets and determining whether the number of buckets should be divided into more buckets or combined into fewer buckets based on comparing the number of buckets to the threshold and as the number of buckets changes, the buckets have values derived from the buckets prior to the change. In Response, the examiner argues that:

> **In response, the examiner agrees with the appellant that Lyle teaches that events that are not related to any other events are associated with a new incident object. Contrarily, events corresponding to an existing event or group of related events are aggregated or combined into a single event. Furthermore, Lyle teaches that as the traffic increases new events are created to accommodate new incidents. However if the traffic corresponds to an existing event, the events will be combined to save resources. At this point, it should be noted that the appellant's claims are broad and interoperated as such. The claimed limitation does not further describe what the threshold is based on, how it is used, etc. In light of this, Lyle teaches the buckets are aggregated/created, divided based on a threshold of how close the incidents relate to one another. Furthermore, event rates and flows received close in time in the same network (yet another threshold) are taken into consideration when creating/dividing/aggregating an event (col 13, lines 19-59). Therefore Lyle meets the scope of the limitation as currently claimed.**

---

[20] Lyle, Col. 19, lines 37-45,
[21] Id. Col. 19, lines 38-45

The examiner misconstrues Lyle, since Lyle does not suggest much less describe "Contrarily, events corresponding to an existing event or group of related events are aggregated or combined into a single event." Appellant has argued above that literally Lyle does not describe that related events are aggregated into a single event, and moreover Appellant has shown that were Lyle to be so interpreted that would make Lyle inoperative. In the quoted passage, Lyle does not aggregate events into a single event, but instead aggregates related events into incidents.

The examiner also argues that: "The claimed limitation does not further describe what the threshold is based on, how it is used, etc." Claim 65 does describe what the threshold is based on – the number of buckets.

The examiner also argues that: "Furthermore, event rates and flows received close in time in the same network (yet another threshold) are taken into consideration when creating/dividing/aggregating an event (col 13, lines 19-59)."

In addition to not teaching aggregated (or accumulated, as called for in base claim 63), Lyle does not teach that event rates or flows are used as thresholds in any comparison of the type claimed in claim 65.

Lyle does not describe or suggest any action of comparing the number of buckets to a threshold number of buckets. Therefore, Lyle does not describe determining whether the number of buckets should be divided into more buckets or combined into fewer buckets based on comparing the number of buckets to the threshold. Lyle also does not describe that as the number of buckets changes, the buckets have values derived from the buckets prior to the change.

Claims 67 and 74

Claim 67 was representative of this group of claims. As far as Appellant can tell, the examiner did not answer Appellant's argument with respect to the features of Claim 67.

Claim 67 includes the feature of accumulating statistic values ... and comparing the values ... to thresholds that depend on the number of buckets. Lyle fails to describe or suggest accumulating statistic values.

3. Claims 1-21, 50-62, 69, and 76-77 are patentable over Lyle in view of Hsu et al.

The examiner summarily answers Appellant's argument regarding the rejection under 35 U.S.C. 103, stating:

> **It should be noted that Lyle does teach a hashing function. Therefore the system of Lyle is able to properly incorporate hashing. Lyle does however fail in determining an integer by applying a hashing function. Hsu teaches using a hashing function to output an integer corresponding to the location of a unique bucket identifier. The examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). The examiner stated in the previous office action that "[I]t would have been obvious to one with ordinary skill in the art at the time the invention was made to combine the disclosure of Lyle with the hashing techniques in Hsu to make the system more efficient. Using the hashing technique, which utilizes addresses, will output the unique bucket identifier quickly. Because Lyle also uses addresses to relate event data to aggregate events into a single incident object, the use of Hsu's hashing technique would work seamlessly." Therefore, not only does Hsu cure the deficiencies of Lyle but would also be seamlessly incorporated into the teachings of Lyle.**

Claims 1 and 7

Claim 1 was representative of this group of claims. Claim 1 calls a machine implemented method of monitoring traffic flow ... and includes the features of producing statistics corresponding to a parameter of traffic flow to trace the source of an attack, ... mapping the traffic flow into a plurality of buckets by applying a hash function "f(h)" to the parameter of the traffic flow to output an integer corresponding to one of the buckets, accumulating statistics from the packets; and comparing the number of buckets to a threshold. The claim also includes determining whether the number of buckets should be divided into more buckets or combined into fewer buckets based on comparing the number of buckets to the threshold.

The examiner does not further argue any teaching from Lyle and for the reasons discussed above and of record these features are not taught by Lyle and Hsu does not cure the

deficiencies in Lyle. For instance Lyle does not suggest the feature of "accumulating statistics from the packets,", as well as analogous features, as argued for claim 63.

Thus, respect to the distinctions of these claims over Lyle and Hsu Appellant relies on Appellant's Appeal Brief.

Motivation to combine

Lyle already uses a hash to assign entries to the queues, a fact overlooked by the examiner[22] and just recently appreciated by Appellant. Lyle teaches:

> **In step 504 the received event data is assigned to a queue by calculating a queue address for the event. In one embodiment, the event manager maintains a table of 21 separate queues configured as three row by seven column table. In one embodiment, the row address is determined by calculating the modulus 3 (MOD 3) of the hash value of the destination address contained in the message or packet. In one embodiment, the column address is calculated by taking the modulus 7 (MOD 7) of the hash value of the entire message or packet. This process would yield a row address between 0 and 2 and a column address between 0 and 6.[23]**

However, that teaching from Lyle, while analogous to the teachings of Hsu and arguably providing motivation to combine with Hsu, still does not meet the claim limitation, since Lyle, like Hsu, discusses the hash in the context of addressing a table. In particular, in Lyle the table is a representation of a queue that awaits logging in a database.

Lyles description of the queue is informative of the underlying distinction between Lyle and Appellant's claims, as expressed of record and above.

In contrast, Claim 1 uses the hash function to map to a bucket that holds accumulating statistical information regarding network packet flows.

Hsu is clearly directed to a table stored in memory and as such requires the use of a technique to distribute entries, e.g., a hash function. As now appreciated by Appellant,[24] Lyle

---

[22] According to the examiner Lyle "Although Lyle does teach the use of hash functions in a unique way to efficiently communicate with the system (see col 19, lines 11-36), however, Lyle does not explicitly indicate the use of a hash function to output an integer corresponding to one of the buckets."

[23] Lyle Col. 11, lines 20-31.

[24] Appellant previously argued that: "Lyle on the other hand is directed to an arrangement in which the incident objects are stored in a database, thus apparently being no such need for a distribution of entries."

However, that argument was based on the examiner's use of the hash teaching in Lyle directed to the communication process disclosed in Col. 19.

has an embodiment directed to a table arrangement for temporary storage of events prior to storage in the logging database and thus also arguably has a need for a distribution of entries.

Therefore, while arguable there may exist suggestion to combine these references, the combination still neither describes nor suggests the claimed features of: "... mapping the traffic flow into a plurality of buckets by applying a hash function "f(h)" to the parameter of the traffic flow to output an integer corresponding to one of the buckets," and accumulating statistics from the packets."

Accordingly, conceding that combination of Lyle and Hsu is suggested, the combination does not describe or suggests the above features of claim 1, and therefore Hsu adds no further teachings to cure the deficiencies in Lyle.

Given this new reading of Lyle, not recognized by the examiner and only now appreciated by Appellant, it is submitted that the remaining claims argued by Appellant are still allowable Lyle and Hsu for the reasons of record, since the combination still does not cure the deficiencies in Lyle. Thus the arguments in Appellant's Appeal Brief, are modified as set out below, to take into consideration suggestion to combine.

Claim 2

Appellant previously argued that:

> Claim 2 limits claim 1 and recites that the buckets are storage areas in memory. Lyle deals with a database and does not specifically discuss buckets as storage areas in memory. While events may reside in memory, temporarily they are ultimately logged into the database taught by Lyle. **Hsu, which does discuss memory, would not cure the deficiencies of Lyle, since it would change the principal of operation of Lyle and is therefore not suggested.[25] (Emphasis added)**

Appellant conceding suggestion to combine Lyle with Hsu withdraws the portion of that argument: "since it would change the principal of operation of Lyle and is therefore not suggested." The remainder of the argument still stands.

---

[25] Appellant's Appeal Brief page 18.

The arguments in Appellant's Brief for Claims 3-6 and 8-13 remain unaffected by the new view of Hsu.

Claims 14, 18, 19, 21, 53, 54, 57, 60, 61, 62, 77

Claim 14 was representative of this group of claims.

Appellant concedes suggestion to combine, as discussed above. Lyle modified by Hsu, still would neither describe nor suggest to map the traffic flow into a plurality of buckets by applying the hash function to the parameter of the traffic flow to output an integer corresponding to one of the buckets and accumulate statistics from the packet.

Accordingly, Hsu adds no further teachings to cure the deficiencies in Lyle and therefore the combination fails to suggest claim 14 for the reasons of record as modified to take into consideration the new view of Hsu.

The arguments in Appellant's Brief for claims 15, 16, 17, 20 and 50, 51, 52, 55, 56, 58, 59, 69 and 76 remain unaffected by the new view of Hsu.

Claims 69 and 76

Claim 69 was representative of this group of claims. Appellant previously argued that:

> **Lyle fails to suggest applying a hash function, as admitted by the examiner and the modification of Lyle with Hsu is not suggested nor provides "mapping the traffic flow into a plurality of buckets comprises applying a hash function "f(h)" to the parameter of the traffic flow to output an integer corresponding to one of the buckets."**

Appellant concedes suggestion to combine Lyle with Hsu and thus withdraws the portion of that argument: "is not suggested." Accordingly, Lyle when combined with Hsu neither describes nor suggests: "mapping the traffic flow into a plurality of buckets comprises applying a hash function "f(h)" to the parameter of the traffic flow to output an integer corresponding to one of the buckets."

Conclusion

For these reasons, and the reasons stated in the Appeal Brief, as modified herein, Appellant submits that the final rejection should be reversed.

Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: 8/30/07

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21723285.doc